IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, **Plaintiff,** **vs.** **BYRON G. MORALES,** **Defendant.**	**8:23CR231** **FINDINGS AND RECOMMENDATION**

This matter is before the Court on the Motion to Suppress and Request for Hearing, and Motion for a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), (Filing No. 38), filed by Defendant, Byron G. Morales. Defendant moves to suppress evidence and statements he made during the course of law enforcement's investigation arising out of a CyberTipline report generated by Facebook. The Government filed a brief opposing Defendant's motion, (Filing No. 53), and Defendant filed a brief in reply (Filing No. 58).

The Court held a telephonic status conference regarding the motion with counsel on November 21, 2024, and held an evidentiary hearing on February 11, 2025. (Filing Nos. 60-61). Defendant was present at the evidentiary hearing with his attorney, Richard McWilliams, and utilized the services of two federally certified Spanish-speaking interpreters. The Government was represented by Assistant United States Attorney, Sean Lynch. Sergeant Stephan Skaar ("Sergeant Skaar") of the Omaha Police Department ("OPD") and Special Agent Buckley Wright ("SA Wright") of the Federal Bureau of Investigation ("FBI") testified on behalf of the Government. At the hearing, the Court received into evidence, without objection, the Government's Exhibits:

Exhibit 1: CyberTipline report #81643543
Exhibit 2: March 16, 2021, Search Warrant Application and Affidavit
Exhibit 3: March 31, 2021, Search Warrant Application and Affidavit
Exhibit 4: Audio recording of Defendant's interview
Exhibit 5: FBI Form FD-941 Consent to Search Computer(s)
Exhibit 6: FBI Form FD-597 Receipt for Property

A transcript (TR.) of the hearing was prepared and filed on February 25, 2025. (Filing No. 68). The record was left open following the hearing for the Government to submit additional evidence in the form of declarations from the NCMEC and Meta. (TR. 68). The Government

submitted the declarations as Exhibits 7 and 8 on March 12 and 17, 2025. (Filing No. 70; Filing No. 75). The matter is now deemed fully submitted. For the following reasons, the undersigned magistrate judge will recommend that Defendant's motion be denied.

BACKGROUND

Defendant is charged in a two-count Indictment with receipt and distribution of child pornography and possession of child pornography under 18 U.S.C. §§ 2252(a)(2), (a)(4)(B), (b)(1), and (b)(2). (Filing No. 1). The charges against Defendant arise out of an investigation that began on October 20, 2020, when Facebook submitted CyberTipline Report #81643543 (hereinafter, "the CyberTip") to the National Center for Missing and Exploited Children ("NCMEC") CyberTipline. (TR. 15; Ex. 1). Sergeant Skaar,[1] a police officer with the Omaha Police Department ("OPD"), was tasked with following up on the CyberTip in his capacity as a task force officer with the FBI. (TR. 14-16). Sergeant Skaar testified that once he receives a cyber tip, he reviews the incident type, the categorizations, how many files NCMEC attached, and the IP address, and then utilizes that information to seek an "unlock warrant" to review the files submitted by NCMEC. (TR. 16).

Sergeant Skaar provided testimony regarding "how cyber tips work." (TR. 23). Cyber tips are triggered by an internet service provider or an electronic service provider, such as Google, Facebook, Instagram, etc., forwarding information to NCMEC. (TR. 23-24). These service providers have "their own repositories of files that have hash values that match what they believe to be contraband," and search their own servers for contraband based upon their hash system that matches hash values against known images. When internet service providers find such contraband, they are required by statute to report it to the NCMEC. (TR. 24-25, 29).

Sergeant Skaar testified he was unsure of what the process entails for the NCMEC to pass files along to law enforcement, as the "state patrol has always been the filter in between me and [NCMEC]." (TR. 26). Sergeant Skaar testified that in this case he received the CyberTip report itself, and the files were transmitted electronically and placed on an external hard drive. (TR. 26-27). Sergeant Skaar testified the CyberTip states NCMEC had not reviewed the files, but he did

[1] Sergeant Skaar has been with the OPD for nearly 11 years, currently working in a supervisory capacity for the child victim sexual assault unit. (TR. 12-13). From the summer of 2020 through the fall of 2021, Sergeant Skaar worked as a task force officer with the FBI conducting investigations arising out of cyber tips from social media platforms. (TR. 13).

not know whether or not anyone from the Nebraska State Patrol viewed the files before transmitting them to him. Sergeant Skaar testified that post-COVID, there is no longer a physical mechanism preventing him from opening the files before obtaining an "unlock" warrant, but that he "still had to go through the process to view them." (TR. 27-28).

Sergeant Skaar testified regarding the information contained in the CyberTip (Ex. 1). The CyberTip states four files were uploaded, indicating the files were "Not Reviewed by NCMEC, Hash Match." The CyberTip explains, "One or more files uploaded in this CyberTipline report have resulted in a 'Hash Match' to a file from a previous CyberTipline report. NCMEC staff have not viewed the uploaded files submitted with this CyberTipline report that are designated as "Hash Match." The 'Hash Match' designation indicates that the uploaded files match the hash values of uploaded files from a CyberTipline report that were previously viewed and categorized by NCMEC at the time this report was generated." On page 2 of the CyberTip, the "incident type" is described as "Anime/Drawing/Virtual." (TR. 17; Ex. 1 at pp. 2, 10). Sergeant Skaar testified an "Anime/Drawing/Virtual" classification would be "Japanese cartoons," drawings, or a computer-generated pornographic image that "does not depict actual children," does not meet the definition of child pornography, and is not illegal to possess. (TR. 29-31). Under "Section A: Reported Information" of the CyberTip, the Incident Information classified the Incident Type as Child Pornography (possession, manufacture, and distribution).[2] (TR. 17; Ex. 1 at p. 4).

The CyberTip identified "Byron Morales [Defendant]," as the suspect, his IP address, information about his Facebook account, and an estimated location in Bellevue, Nebraska. (Ex. 1 at p. 4). Section A also provided "Uploaded File Information" for each of the four files provided by the electronic service provider ("ESP"). The upload information for the first file stated, "This image was uploaded because it was sent three messages before Child Exploitation imagery (CEI)"; the second file states, "This image was uploaded because it was sent immediately before Child Exploitation Imagery (CEI)"; the third file states, "This is the profile picture for the account[]"; and the fourth file is an .mp4 file categorized by reporting ESP as "B1." The reporting ESP did not provide information as to whether or not it viewed the entire contents of the three non-CEI

[2] In other words, the CyberTip inconsistently described the incident in some places as "Anime/Drawing/Virtual," which Sergeant Skaar understood to be legal to possess, but as child pornography or child exploitation imagery in others, which Sergeant Skaar understood to be illegal to possess. (TR. 18, 23, 31).

files, and indicated "No," it did not review the entire contents of the file it categorized as B1. (TR. 33; Ex. 1 at pp. 5-6).

Section B in turn contains a table categorizing flagged images. Sergeant Skaar testified this table was "significant" because the image categorization was "B1," which is "a pubescent minor engaging in a sex act." (TR. 17-18; Ex. 1 at p. 8). Sergeant Skaar testified this categorization is "Facebook's interpretation of what it thinks it's passing along [to NCMEC]" and not a categorization by anyone at NCMEC. (TR. 38-39).

Section C of the CyberTip contains "Additional Information Provided by NCMEC." The NCMEC classification is again listed as "Anime/Drawing/Virtual," and indicates "Files Not Reviewed by NCMEC, Hash Match." (Ex. 1 at p. 10; TR. 42-43). Section C reiterates that "NCMEC staff have not viewed the following uploaded files submitted with this report and have no information concerning the content of the uploaded files other than information voluntarily provided in the report by the reporting ESP." (*Id.*).

Based upon the above CyberTip, Sergeant Skaar prepared a search warrant affidavit and application on March 16, 2021, to open and review the four files on the external hard drive from CyberTip #81643543 from NCMEC. (TR. 18; Ex. 2). The affidavit and application contained the following information:

> 1. The National Center for Missing and Exploited. Children (NCMEC), headquartered in Alexandria, Virginia, is a 50l(c)(3) nonprofit organization. The NCMEC website (www.missingk.ids.com) states: "Established in 1984, the [NCMEC] is the leading nonprofit organization in the U.S. working with law enforcement, families and the professionals who serve them on issues related to missing and sexually exploited children." Pursuant to a congressional mandate, NCMEC launched its CyberTipline in 1998. 42 U.S.C. § 5773(b) authorizes and funds NCMEC's operation of a cybertipline to provide online users an effective means of reporting Internet-related child sexual exploitation.
>
> 2. Federal law mandates that all electronic communication service or remote computer service providers report all facts or circumstances from which there is an apparent violation of federal child pornography laws to the CyberTipline. 18 U.S.C. § 2258A. Federal law provides in pertinent part that "'child pornography' means any visual depiction of sexually explicit conduct, where - (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct." 18 U.S.C. § 2256(8). A "'minor" means any person under the age of eighteen years." 18 U.S.C. § 2256(1). Federal law provides in pertinent part that "'sexually explicit conduct" means actual or simulated - (i) sexual intercourse. including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic

or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person." 18 U.S.C. § 2256(2)(A). Some electronic communication service and remote computer service providers have their own databases of previously-identified files; some of these files may contain depictions that do not constitute child pornography under federal law.

3. This investigation began on October 20th, 2020, when Facebook submitted CyberTipline Report# 81643543 to the NCMEC CyberTipline. This report was the result of a hash value match on at least one digital image attached to an electronic message sent to an identified Facebook Messenger account. Specifically, [jaKQhG9Ud7ZVDvXl10000000_4452547168153343_493944~757754S386_n.mp4]. When making its report to the CyberTipline, Facebook listed "Information not Provided by Company" when asked if the reporting ESP viewed the entire contents of the uploaded file. It is assumed rather, Facebook relied on the hash value match to identify the Child Sexual Exploitation Material.

4. Your affiant has learned that Facebook has a process in place to detect whether a known file of child pornography is being sent or received via a Facebook account. Facebook maintains a database of hash values for files that Facebook has determined constitute child pornography, and uses that database to automatically compare files that are sent through a Facebook account. "A hash value is an alphanumeric sequence that is unique to a specific digital file. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Consequently, once a file has been 'hashed,' a suspected copy can be determined to be identical to the original file if it has the same hash value as the original, and not to be identical if it has a different hash value." *United States v. Keith*, No 11-10294 (D. Mass, Nov. 5, 2013), 2013 WL 5918524 at * 1. When Facebook detects a file passing through its servers with the same hash value of a file from its database of known child pornography, Facebook submits a report to the CyberTipline for the [NCMEC] as required by 18 U.S.C. § 2258A(a)(l). In making the report, Facebook electronically uploads to NCMEC a copy of the file attachments, along with the IP address used to send the communication.

5. In making this affidavit, I am aware of the decision by the federal district court in *United States v. Keith*, No 11-10294 (D. Mass, Nov. 5, 2013), 2013 WL 5918524. In that case, a federal district court held that the NCMEC acted as a government agent when a NCMEC analyst opened and viewed an electronic mail attachment that an internet service provide[r] had forwarded to the NCMEC as suspected child pornography. In *Keith*, the court found that the NCMEC's opening of the electronic mail attachment without a search warrant violated the Fourth Amendment. *Id.* at *12. Although *Keith* is not controlling in this district and there is reason to question its reasoning, in an abundance of caution, I will not describe in this affidavit the result of the NCMEC and [law enforcement] review of the images. I ask the court

> to draw no inferences from the fact that [NCMEC and/or law enforcement] opened and viewed the electronic mail message and the attachment(s).[3]
>
> 6. On December 8th, 2020, Affiant Officer [Skaar] was assigned CyberTip #81643543 for investigation. A/O reviewed the CyberTip which included four (4) files submitted by Facebook along with identifiers for the subject account. Facebook provided the name Byron Morales as the username for the account which allegedly uploaded the child exploitation imagery. Facebook also provided the phone number [ending in -3728], the date of birth -1973 and the profile URL address for [Defendant's] account. . . .
>
> 7. Upon receiving the CyberTip, the Nebraska State Patrol had already submitted a subpoena to Verizon Wireless for the phone number associated with the Facebook account [-3728]. A/O reviewed the response sent by Verizon Wireless which stated the account belonged to a Byron Morales at the address [11th Street].
>
> 8. A/O located a Byron Morales on NCJS with a date of birth -1969 who has the address of [] 11th Street Omaha, NE 68108 listed on his Nebraska Driver's License.

(Ex. 2 at pp. 1-5). A Douglas County County Court Judge issued a warrant authorizing the search and seizure of the contents and attachments of the CyberTip based on the foregoing affidavit. (Ex. 2 at p. 5).

Sergeant Skaar testified he does not specifically recall why he did not include the information that the CyberTip referred to the "incident type" as "Anime/Drawing/Virtual" in his affidavit, but he "imagine[d]" it was because he "didn't think anything of it or I was basing it solely off the rest of the information in the report, which states it was child pornography possession and then the categorization of a B1." (TR. 18-19). Sergeant Skaar testified he was "focusing on what was contained in Section A and Section B of the [CyberTip]." (TR. 19). Sergeant Skaar testified he did not intentionally decide to omit the information that the CyberTip referred to the "incident

---

[3] On cross-examination, defense counsel asked Sergeant Skaar about paragraph 5 of his affidavit:

> Q. So what you are saying there, effectively, is that NCMEC and/or law enforcement opened and viewed the electronic mail message and the attachments; is that accurate?
> A. I don't know that I understand it that way.
> Q. Well, it says: I ask the court to draw no inferences from the fact that NCMEC and/or law enforcement opened and viewed the electronic mail message and the attachments.
> A. Right. Yeah. It does appear it reads that way.

(TR. 49). Sergeant Skaar later testified he did not open the images contained within the CyberTip prior to obtaining a warrant. (TR. 52). In an affidavit authored on February 28, 2025, by Fallon McNulty, a Director with the CyberTipline for the Exploited Children Division, McNulty also clarified, "NCMEC staff did not view the four (4) uploaded files" as stated in the CyberTip. (Ex. 7 at p. 3).

type" as "Anime/Drawing/Virtual." (TR. 22). Sergeant Skaar testified that, because he had not reviewed the images, he did know which classification was correct or not. (TR. 31). Sergeant Skaar testified his search warrant application referred to the content as "child exploitation imagery" because that "is how it's referred to multiple times throughout the cyber tip. They call it child exploitation imagery, and then throughout they called it CEI." (TR. 20). Sergeant Skaar testified his understanding of the term "child exploitation imagery" or "child sex exploitation imagery" is that it is interchangeable with "child pornography" under federal law, and would not encompass legal images. (TR. 37, 48). Sergeant Skaar testified he would not use "virtual child pornography" and "child exploitation imagery" interchangeably. (TR. 38). Sergeant Skaar testified he did not think the ESP would categorize a cartoon-pubescent-minor engaging in a sex act as "B1," and believed only images containing actual minors would be categorized as such. (TR. 40-41).

In an affidavit authored on February 28, 2025, by Fallon McNulty, a Director with the CyberTipline for the Exploited Children Division ("ECD"), McNulty explained, "When Facebook submitted the report [to NCMEC] on October 20, 2020, "Facebook indicated the Incident Type as "Child Pornography." NCMEC generated CyberTipline report #81643543 upon receipt of Facebook's report. McNulty averred that, "When processing CyberTipline report #81643543, the classification 'Anime/Drawing/Virtual' was incorrectly assigned to CyberTipline report #81643543. Upon subsequent review, NCMEC amended the classification of CyberTipline report #81643543 to 'Apparent Child Pornography.'" (Ex. 8 at pp. 1-2).

Sergeant Skaar did not open the images contained within the CyberTip prior to obtaining the warrant. (TR. 52). After the warrant was issued, Sergeant Skaar viewed the contents of the CyberTip files. At least one of the files depicted a 10- to 12-year-old female child engaging in sexually explicit conduct. (TR. 21).

Sergeant Skaar subsequently obtained a search warrant through Douglas County Court to access the Facebook account of Defendant. (TR. 21-22; Ex. 3). The search warrant affidavit, dated March 31, 2021, contained the information that on October 20, 2020, Facebook submitted CyberTipline Report #81643543 to NCMEC "as they had flagged an account on their service for uploading apparent child pornography" and connected it to Defendant's Facebook account. The affidavit continues, "As stated in NCMEC CyberTipline Report #81643543, the Facebook profile in question sent three files believed to contain child exploitation material to another user on

Facebook Messenger . . . Facebook Inc. attached the files with their report along with the suspect's profile picture for the account. A/O wrote a search warrant to view the attached files as the information had not been provided by Facebook regarding if they had previously viewed the files or not." (Ex. 3 at p. 3). The affidavit states that, after a search warrant was issued, "A/O reviewed one of the files which was an mp4 video," and described the contents of the video, which depicted a 10- to 12-year-old female child engaging in a sexually explicit act. The next file was described as a photo depicting a "juvenile female approximately 6-9 years of age, seated with her hand down the front of her underwear"; the next file was "a picture of a clothed juvenile female seated on a bed;" and the fourth file was the suspect's account's profile picture. The affidavit described how data from social media applications can assist investigators and the type of data sought by the warrant. A Douglas County Court judge authorized the warrant on March 31, 2021. (Ex. 3 at pp. 3-5). There is no information before the Court regarding what, if any, evidence was obtained as a result of this warrant.

It appears the investigation stalled for a period of time until SA Wright became involved mid-2023 after Sergeant Skaar left the FBI task force. SA Wright works with the FBI primarily investigating crimes against children. (TR. 56). At the time SA Wright took over the investigation, Sergeant Skaar had completed the review of Defendant's Facebook account. (TR. 57-58). On July 7, 2023, SA Wright sought to interview Defendant. SA Wright, accompanied by a Spanish-speaking agent, Special Agent Thane Palmer ("SA Palmer"), both wearing plain clothes, first attempted to locate Defendant at his residence before going to his place of employment, an auto mechanic supply store. (TR. 58-60). Defendant was working at the checkout counter. Defendant spoke to the agents in English, and the agents observed Defendant speaking to customers in English. The agents identified themselves and Defendant agreed to speak to them. (TR. 60, 74).

SA Wright asked Defendant if there was a more private place to talk, and Defendant took the officers to the employee break room. SA Wright testified the breakroom was "fairly small,"—about 10x10—with a table and a couple chairs. The agents sat one side of the table and Defendant sat on the other. SA Wright testified that although the breakroom door was shut, the agents were not blocking Defendant and were not positioned between Defendant and the door. (TR. 61, 75). SA Wright conversed with Defendant in English throughout the interview; SA Wright testified Defendant never expressed confusion or asked for an interpreter, and his answers were consistent with the questions being asked. (TR. 63-64). Defendant was "in his 50s or 60s" at the time of the

interview and did not appear intoxicated. Defendant did not ask to speak in Spanish and specifically stated he is able to speak English. (TR. 70).

SA Wright commenced the interview at 4:46 p.m. and audio-recorded the conversation. (TR. 62; Ex. 4). At the outset, SA Wright advised Defendant that he was free to leave and that he was not required to talk to them, but did not provide a formal *Miranda* rights advisement. (TR. 63). The agents discussed Defendant's Facebook account, the nature of the cyber tips and Defendant's involvement with that type of conduct. SA Wright asked if Defendant still had any of that material on his device. Defendant took out his phone and "displayed his phone and provided for agents to review it," during which SA Wright observed apparent child pornography. (TR. 64, 76; Ex. 4 at 14:00-16:30).

Approximately 40 minutes into the interview, Defendant asked for a break to help his coworkers close up the business. SA Wright told Defendant he was going to let him go, but said, "since you have those images and videos on your phone, that is illegal," and that he was "going to have to take this phone with me today." (Ex. 4 at 40:10-53). SA Wright testified he intended to retain possession of Defendant's phone "due to the nature of the content that was located on it," i.e., the apparent child pornography he had observed. (TR. 65, 76). SA Wright admittedly did not have consent or a warrant to seize Defendant's cell phone. (TR. 77).

SA Wright asked Defendant if he would be "willing to sign a form to let me search your phone." Defendant hesitated because he "really need[s]" his phone. SA Wright replied, "It's your decision," and informed Defendant that giving such consent would not lead to him getting his phone back sooner. (Ex. 4 at 41:05-42:36; TR. 66-67). SA Wright testified he advised Defendant "multiple times" he was free to decline consent to search, and that providing consent "would not get his phone back quicker." (TR. 66-67). Defendant asked SA Wright if he was charged with something and expressed concern about losing his job, and SA Wright replied, "that's tough to tell" and will "largely . . . depend on what else we find on the phone." (Ex. 4 at 44:48-45:40).

SA Wright told Defendant he could go finish his tasks for work, and indicated that when he was done they could "finish talking" and Defendant could call who he needed to before the agents took his phone. SA Wright asked Defendant "if that works," and Defendant replied, "yeah." The agents then went outside to wait in the parking lot near their plain, unmarked vehicle. (TR. 64-65, 74; Ex. 4 at 46:00-25).

About ten minutes later Defendant reapproached the agents, who were outside in the parking lot near their vehicle. To SA Wright's knowledge, Defendant's vehicle was located in a separate area of the parking lot. (Ex. 4 at 56:30; TR. 65-66). SA Wright told Defendant they were going to have to take his phone "for a long time," that prosecutors would be the ones to determine whether to bring charges against him, and that SA Wright does not have any control over whether or not he keeps his job. SA Wright told Defendant the next time Defendant sees him it would be to either return his phone or to arrest him, "down the road" and "probably six plus months," but that this is "by no means the end of your life." Defendant replied, "It is, I've never been in jail," and SA Wright stated, "Nobody said you're going to jail." Defendant asked, "Do I need a lawyer?" and SA Wright replied, "That's up to you. I can't give you advice." (Ex. 4 at 56:30-58:45).

SA Wright and Defendant continued to talk and wrap up the interview for another approximately ten minutes before SA Wright returned to his request for Defendant's consent to search his phone. SA Wright explained that without consent, he would have to get a search warrant that a judge "signs off on." SA Wright explained that taking Defendant's phone is different from searching his phone and he "can't look at it" without consent or a warrant. SA Wright continued, "I need you to give me consent to say I can look at it, or I need to go get a search warrant from a judge." Defendant responded, "I'll sign it, whatever" and repeated, "You already got it," referring to SA Wright's seizure of the phone; SA Wright again clarified, "I got it, but I can't search it." (Ex. 4 at 1:08-1:09:40).

SA Wright prepared a Form FD-597 property receipt for Defendant's cell phone, explaining the form's purpose and explained it is not the consent form. (TR. 69-70; Ex. 6 at 1:09:59-1:10:40). SA Wright next provided Defendant with Form FD-941, the FBI's consent to search computers or cell phones form. SA Wright explained to Defendant he would read the form out loud while Defendant reads along; Defendant indicated he has a college degree and can read, "Otherwise I'd be working in a factory." SA Wright read the form to Defendant, and summarized that, "In short it's saying that you are giving the FBI consent to search this phone and take any evidence that we find in it. If you consent to that, you sign right there." Defendant then signed the form consenting to the search of his Samsung Galaxy cell phone. SA Wright asked Defendant if he had any final comments, questions or concerns, thanked Defendant for his cooperation, and terminated the interview and let Defendant leave. (TR. 67-69; Ex. 4 at 1:11:42-1:16:30; Ex. 2).

The Indictment in this matter was returned on November 14, 2023. (Filing No. 1). Defendant has filed the instant motion seeking suppression of all evidence seized and statements he made during the course of the investigation. Defendant moves to suppress on five grounds: (1) the warrantless search of his Facebook account by Facebook, a government agent, the NCMEC, a government entity, and law enforcement violated his Fourth Amendment rights; (2) the March 16, 2021, search warrant application was facially insufficient to support probable cause; (3) the March 16 and 31, 2021, search warrant applications contained factual omissions and/or misstatements requiring a hearing under *Franks*; (4) "The poisonous tree yielded many fruits"; and (5) Defendant made incriminating statements involuntarily and did not provide valid consent for law enforcement to seize and search his cell phone. (Filing No. 39; TR. 80).

The Government counters that Facebook is not a governmental entity and did not conduct a warrantless search in violation of the Fourth Amendment by forwarding the CyberTip to NCMEC based upon the hash values match of the file, (Filing No. 53 at p. 7); Defendant did not make a substantial preliminary showing for a *Franks* hearing, (Filing No. 53 at p. 9); that the *Leon* good faith exception would apply even assuming there was a Fourth Amendment violation, (Filing No. 53 at p. 10); Defendant's statements during his interview were voluntary (Filing No. 53 at p. 11); and Defendant validly consented to the search and seizure of his phone (Filing No. 53 at p. 13).

ANALYSIS

I. Defendant's Pre-Warrant Constitutional Challenges

Defendant argues that his Fourth Amendment rights were violated at the inception of this investigation when Meta (Facebook)—a government agent—"review[ed] and forward[ed]" Defendant's Facebook files to NCMEC—a government entity—"under both a reasonable-expectation-of-privacy and a trespass-to-chattels theory of the amendment." (Filing No. 39 at pp. 1-3).

The Fourth Amendment only applies to state action and its protection against unreasonable searches and seizures "is wholly inapplicable to a search or seizure . . . effected by a private individual not acting as an agent of the Government." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). "Whether a private party should be deemed an agent or instrument of the government for Fourth Amendment purposes necessarily turns on the degree of the government's participation

in the private party's activities, a question that can only be resolved in light of all the circumstances." *United States v. Ringland*, 966 F.3d 731, 735 (8th Cir. 2020) (quoting *United States v. Wiest*, 596 F.3d 906, 910 (8th Cir. 2010)). "A defendant bears the burden of proving by a preponderance of the evidence that a private party acted as a government agent." *Id.* (quoting *United States v. Highbull*, 894 F.3d 988, 992 (8th Cir. 2018)).

As previously discussed by the Eighth Circuit, an internet service provider's fulfillment of child pornography reporting requirements under 18 U.S.C. § 2258A, standing alone, "does not transform an internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography." *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013) (concluding AOL did not act as a government agent when it scanned a user's e-mail using its hash-detection program and reported apparent child pornography to NCMEC).

In *Ringland*, the Eighth Circuit rejected the same argument advanced by Defendant in this case, specifically, that an electronic service provider, Google, did not act as a government agent because it was "coerced into reporting child pornography by statutory penalties imposed for failing to report such content." 966 F.3d at 736. In *Ringland*, Google's hash-comparison technology detected several hundred child pornography files in the defendant's gmail account. Google then reviewed hundreds of those the files before sending a CyperTipline Report to NCMEC. The Eighth Circuit found that "Google did not act as a government agent because it scanned its users' emails volitionally and out of its own private business interests," as Google and the government have a "mutual interest in eradicating child pornography from its platform." *Ringland*, 966 F.3d at 736. Google performed the initial scans of the defendant's email account without the government's knowledge, the government did not request the searches, and "Google acted out of its own obvious interests in removing child sex abuse from its platform." And while 18 U.S.C. § 2258A imposes a reporting requirement, the Eighth Circuit determined "the statutory scheme does not so strongly encourage affirmative searches such that it is coercive," and in fact "may even discourage searches in favor of willful ignorance." *Ringland*, 966 F.3d at 736. Therefore, the Eighth Circuit concluded "Google was not a state actor here and its searches do not implicate the Fourth Amendment." *Id.*

In this case, like in *Ringland*, Defendant argues Meta (formerly Facebook) acted as a government agent because 18 U.S.C. § 2258A(a)(1) imposes penalties upon internet service providers for failing to report child pornography content. (Filing No. 39 at pp. 2-3). Defendant appears to recognize this position has been foreclosed by the Eighth Circuit Court of Appeals in

Ringland. See Filing No. 39 at p. 3 ("Nonetheless, the Eighth Circuit has held searches by electronic-service providers (ESPs) are private.") (citing *Ringland*, 966 F.3d 737).

After review of the relevant binding precent and the circumstances of this case, the undersigned magistrate judge finds and concludes Meta did not act as a government agent in using its hash-value system to identify the and forward child pornography from Defendant's Facebook account to NCMEC. Meta, like Google, is a private company providing internet services to its users. Meta's Community Standards provide, "We do not allow content or activity that sexually exploits or endangers children. When we become aware of apparent child exploitation, we report it to the National Center for Missing and Exploited Children ('NCMEC'), in compliance with applicable law." Meta declared it "has a strong business interest in enforcing our terms of service and ensuring that our services are free of illegal content, including, in particular, child sexual abuse material" and that they "independently and voluntarily take steps to monitor and safeguard our services against this content because users will stop using our services if they become associated with being a haven for abusive content. Ridding our services of CSAM is thus, critically important to protecting our users, products, brand, and business interests." Based upon those private interests, "Meta identifies content that might violate its Community Standards," and if Meta "discovers apparent child pornography as defined in 18 U.S.C. § 2256, Meta provides a report to NCMEC via the CyberTipline in accordance with its statutory obligation under 18 U.S.C. § 2258A." (Ex. 8). The record establishes Meta independently monitors its services out of its own private business interest in ridding its services of illegal content, including child sexual abuse material. There is no evidence the government knew of Meta's initial scan of Defendant's Facebook account or that the government requested the search. Therefore, the undersigned magistrate judge finds Meta was a private party, not a government agent. Because Meta was not a government agent, its search (to the extent its hash-matching identification of files on its platform without reviewing the files constitutes a search) does not implicate the Fourth Amendment.

Defendant next argues that NCMEC, a government entity (or at a minimum, a government agent), violated the Fourth Amendment by "taking the files from [Meta], analyzing and investigating them, and then forwarding them to law enforcement." (Filing No. 58 at p. 1). Defendant contends *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016) is implicated because "any analysis done by NCMEC is a, per se, expansion of what [Meta] has done," thereby either expanding upon [Meta]'s private search in violation of *Ringland* and *Stevenson*, or

independently violating the Fourth Amendment under a "trespass-to chattels property-based *Jones* test" under *United States v. Jones*, 565 U.S. 400, 404-05 (2012). (TR. 80; Filing No. 58 at p. 4).

"If a private party conducted an initial search independent of any agency relationship with the government, then law enforcement officers may, in turn, perform the same search as the private party without violating the Fourth Amendment as long as the search does not "exceed[ ] the scope of the private search." *Ringland*, 966 F.3d at 736 (quoting *United States v. Miller*, 152 F.3d 813, 815 (8th Cir. 1998)). "This is because the private search already frustrated the person's legitimate expectation of privacy; thus, 'an ensuing police intrusion that stays within the limits of the private search is not a search for Fourth Amendment purposes.'" *Id.* (quoting *Miller*, 152 F.3d at 815). Defendant relies on *Ackerman*, 831 F.3d 1292, wherein the Tenth Circuit concluded that NCMEC is a government agent that violated the Fourth Amendment by expanding the scope of a private internet service provider's investigation without a warrant. In *Ackerman*, the undisputed facts established that NCMEC opened and viewed information other than the image flagged by AOL's hash values as known child pornography and had not been previously examined by AOL. Therefore, the Tenth Circuit found that NCMEC exceeded, and did not merely repeat, the internet service provider's private search in violation of the Fourth Amendment. See *Ackerman*, 831 F.3d at 1306-07; see *United States v. Boyer*, 914 F.2d 144, 146 (8th Cir. 1990) ("[T]he government may not exceed the scope of the private search unless it has the right to make an independent search[.]"). Conversely, in *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018), the Fifth Circuit found that law enforcement did not violate the Fourth Amendment because the investigator "reviewed only those files whose hash values corresponded to the hash values of known child pornography images" as ascertained by the internet service provider's system. *Id.* at 640.

Separate from the private party search issue involving an infringement upon a reasonable expectation of privacy, Defendant advances the argument that NCMEC, a government entity (or agent), also violated the Fourth Amendment by the "warrantless opening and examination of files that could have contained much besides contraband" constituting a "trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment." (Filing No. 39 at p. 5; TR. 82). Defendant derives this argument from *Ackerman*, which recognized that "government conduct can constitute a Fourth Amendment search *either* when it infringes on a reasonable expectation of privacy or when it involves a physical intrusion (a trespass) on a constitutionally protected space or thing ("persons, houses, papers, and effects") for the purpose of obtaining

information." *Ackerman*, 831 F.3d at 1307 (emphasis in original) (discussing *United States v. Jones*, 565 U.S. 400 (2012)). The Tenth Circuit in *Ackerman* concluded, "whether we analyze the 'search' question through the lens of the government's preferred authority—*Jacobsen* and *Katz*—or through the lens of the traditional trespass test suggested by *Jones*, they yield the same (and pretty intuitive) result: NCMEC conducted a 'search' when it opened and examined [Defendant's] email." *Ackerman*, 831 F.3d at 1307 ("We are dealing instead with the warrantless opening and examination of (presumptively) private correspondence that could have contained much besides potential contraband for all anyone knew. And that seems pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment.").

Relevant to both Fourth Amendment violation arguments advanced by Defendant above, in this case, the undersigned magistrate judge finds that the evidence establishes the following facts: (1) Meta, a private party, identified one file containing an image of sexually explicit conduct involving a pubescent minor on Defendant's Facebook account using Meta's hash value system; (2) Meta did not review the entire contents of the uploaded files (See Ex. 1); (3) Meta submitted a report to NCMEC indicating it had identified child pornography on its platform by hash match; (4) NCMEC generated CyberTipline report #81643543 upon receipt of Meta's report; (5) Meta uploaded four (4) files in CyberTipline report #81643543, one of which was publicly available, one of which was identified as child exploitation imagery by hash match, and two others which were sent due to their immediate proximity to the hash matched file; (6) "NCMEC staff did not view the four (4) uploaded files," (See Ex. 7); (7) the "Hash Match" designation indicates that the uploaded files match the hash values of uploaded files from a CyberTipline report that were previously viewed and categorized by NCMEC at the time this report was generated; and (8) Sergeant Skaar did not review the files transmitted from NCMEC to the Nebraska State Patrol until a judge issued the "unlock warrant" on March 16, 2021 (TR. 52). In other words, the evidence before the Court establishes that Facebook, NCMEC, and law enforcement did not actually open and view the four files prior to the authorization of the "unlock" warrant. Instead, only the file name and hash value match were known to NCMEC and law enforcement prior to obtaining a warrant.

Defendant, recognizing the significance of this distinction, argues "that even though other courts, like the Eighth Circuit, have drawn some legal niceties between the hash value comparison

and review of a file, those are effectively the same thing" because "If you know that this hash value contains a certain image and you look at the hash value, you are effectively reviewing the image." (TR. 81). The undersigned magistrate judge disagrees that this distinction is legally insignificant. *Ackerman*, *Ringland*, and *Reddick* all involve fact patterns where NCMEC, law enforcement, or both, actually "opened and examined [Defendant's] email" without a warrant. While the Fourth Amendment discussion may become murkier had someone at NCMEC or law enforcement opened the files before obtaining a warrant, here, the record does not establish that either NCMEC or law enforcement opened and reviewed any of the four files prior to obtaining a warrant.

Instead, NCMEC identified the child pornography file by hash match alone, meaning the uploaded file "match[ed] the hash values of uploaded files from a CyberTipline report that were previously viewed and categorized by NCMEC at the time this report was generated." Meta's hash technology had already "searched" the actual contents of the file and learned what the corresponding hash value was, which was then provided to NCMEC, and that the hash value of the uploaded file matched the hash value of was an exact match for an image that was already contained in NCMEC's database. See, e.g., *United States v. Holmes*, 121 F.4th 727, 745 (9th Cir. 2024) (Collins, J., dissenting) ("To use an analogy, what Facebook did was akin to enclosing a book in a sealed envelope and submitting it to the Library of Congress with a statement that the enclosed book corresponds to a specific Library of Congress classification number; by consulting its own collection, the Library would be able to know exactly what the contents of the book are, even without breaking the seal. . . . Facebook's submission [to NCMEC] effectively disclosed the precise contents of the file to the Government, without any need to open the uploaded image file. Consequently, any 'expectation of privacy' in that image had "already been frustrated."). Defendant has not provided the Court with evidence or caselaw suggesting that hash matching alone, without opening and viewing the contents of the files, is violative of the Fourth Amendment. See *Reddick*, 900 F.3d at639 ("[W]hatever expectation of privacy [the defendant] might have had in the hash values of his files was frustrated by [the ESP's] private search."). Therefore, the undersigned magistrate judge finds that Defendant's Fourth Amendment rights were not violated in connection with the CyberTip in this case.

II. Defendant's challenges to the search warrants

a. Material omissions/Franks request

Defendant argues he is entitled to a *Franks* hearing because material facts were intentionally omitted from the March 16 and March 31, 2021, search warrant applications, and because the applications included information and evidence that had been obtained through unconstitutional warrantless searches by Facebook and NCMEC in violation of the Fourth Amendment. (Filing No. 39 at pp. 1-10).

A criminal defendant may request a hearing to challenge a search warrant on the ground that the supporting affidavit contains factual misrepresentations or omissions relevant to the probable cause determination. See *Franks*, 438 U.S. at 155-56. In order for a defendant to prevail on a request for a *Franks* hearing, the defendant must make a "substantial preliminary showing" that (1) the affiant "knowingly and intentionally" made reckless false statements or omissions and (2) if the false information is excised (or the omitted information is included), the affidavit no longer establishes probable cause. *United States v. Snyder*, 511 F.3d 813, 816 (8th Cir. 2008).

Recklessness may be "inferred from the fact of omission of information from an affidavit . . . when the material omitted would have been 'clearly critical' to the finding of probable cause." *United States v. Williams*, 477 F.3d 554, 559 (8th Cir. 2007) (quoting *United States v. Reivich*, 793 F.2d 957, 961-62 (8th Cir. 1986)); see also *United States v. Jacobs*, 986 F.2d 1231, 1235 (8th Cir. 1993) (stating that an officer acts recklessly by withholding information that "[a]ny reasonable person would have known that this was the kind of thing the judge would wish to know"). Recklessness may also be inferred, when after viewing all the evidence, it is clear that the affiant "must have entertained serious doubts as to the truth of his statements or had obvious reasons to doubt the accuracy of the information he reported." *United States v. McIntyre*, 646 F.3d 1107, 1114 (8th Cir. 2011) (citation omitted). "Allegations of negligence or innocent mistake will not suffice." *United States v. McIntyre*, 646, F.3d 1107, 1114 (8th Cir. 2011).

In the case of an omission, suppression is appropriate "only if the affidavit as supplemented by the omitted material could not have supported the existence of probable cause." *United States v. Lueth*, 807 F.2d 719, 726 (8th Cir. 1986) (emphasis in original). In either case, the Court must void the search warrant and exclude the fruits of the search "to the same extent as if probable cause was lacking on the face of the affidavit." *Franks*, 438 U.S. at 156. "The requirement of a

substantial preliminary showing is not lightly met[.]" *United States v. Arnold*, 725 F.3d 896, 898 (8th Cir. 2013) (quoting *United States v. Mathison*, 157 F.3d 541, 548 (8th Cir. 1998)).

Defendant argues the following omissions from the March 16, 2021, warrant application necessitate a hearing under *Franks*: (1) NCMEC's classification of the incident as "Anime/Drawing/Virtual;" (2) two of the files had been sent by Facebook to NCMEC merely because the images were sent "three messages before" or "immediately before" "child exploitation imagery;" (3) that one of the four files "was a user-profile picture – obviously not contraband at all"; and that (4) that there was a substantial possibility that the files did not meet 18 U.S.C. § 2256's definition of "child pornography."

At first blush, the undersigned magistrate judge would tend to agree with Defendant that the March 16, 2021, search warrant application omitted information relevant to the probable cause finding. Arguably, the issuing judge may have found it relevant that the CyberTip inconsistently described the incident "as "Anime/Drawing/Virtual" in some places, which classification Sergeant Skaar testified does not meet the definition of child pornography and is not illegal to possess, while simultaneously indicating the incident was child pornography or child exploitation imagery in others, which Sergeant Skaar understood to be illegal to possess. (TR. 18, 23, 29-31). The Anime/Drawing/Virtual description may have been particularly relevant to the warrant application in this case because neither Facebook nor NCMEC actually reviewed the files to confirm their contents; instead, probable cause was based upon hash value identification alone. NCMEC submitted an affidavit after the evidentiary hearing in this matter indicating the misclassification was an error on its end; when Facebook submitted the report to NCMEC, Facebook indicated the incident type was "Child Pornography," but NCMEC incorrectly assigned the Anime/Drawing/Virtual classification when processing the CyberTip. NCMEC has since amended the classification to "Apparent Child Pornography." (Ex. 8 at pp. 1-2). Clarification of that error could have, and probably should have, been done prior to seeking a warrant.

Nevertheless, the undersigned magistrate judge finds and concludes that the omission of that information, along with the other information cited by Defendant, was not intentional or reckless (nor "clearly critical" to the finding of probable cause), and was at most negligent. See *McIntyre*, 646, F.3d at 1114 ("Allegations of negligence or innocent mistake will not suffice."). Sergeant Skaar testified he does not specifically recall why he did not include the information that the CyberTip referred to the "incident type" as "Anime/Drawing/Virtual" in his affidavit, but he

"imagine[d]" it was because he "didn't think anything of it or I was basing it solely off the rest of the information in the report, which states it was child pornography possession and then the categorization of a B1." (TR. 18-19). Sergeant Skaar testified Facebook's categorization of the file as "B1" means it depicts "a pubescent minor engaging in a sex act." (TR. 17-18; Ex. 1 at p. 8). Sergeant Skaar testified he did not think Facebook would categorize a cartoon-pubescent-minor engaging in a sex act as "B1," and believed only images containing actual minors would be categorized as such. (TR. 40-41). Sergeant Skaar testified he was "focusing on what was contained in Section A and Section B of the [CyberTip]." (TR. 19). Sergeant Skaar testified he did not intentionally decide to omit the information that the CyberTip referred to the "incident type" as "Anime/Drawing/Virtual." (TR. 22). Sergeant Skaar further testified his understanding of the term "child exploitation imagery" or "child sex exploitation imagery" is that it is interchangeable with "child pornography" under federal law, and would not encompass legal images. (TR. 37, 48). Sergeant Skaar testified he would not use "virtual child pornography" and "child exploitation imagery" interchangeably. (TR. 38). Given the accuracy and reliability of hash matches and Sergeant Skaar's testimony regarding his understanding of the terms used by Facebook and NCMEC, the undersigned magistrate judge finds he did not recklessly or intentionally omit information from his warrant application.

The undersigned also finds it was not a *Franks* violation to omit specific information about the other three files forwarded by Facebook to NCMEC. As argued by the government at the evidentiary hearing, Facebook forwarded two other files "that preceded or were in proximity to the [hash match] video in question being sent as well as the profile picture," which could provide context or also constitute evidence of a crime due to its immediate proximity to the crime of child pornography. (TR. 88).

b. Facial validity/good faith reliance on March 16, 2021, warrant

Defendant challenges the validity of the March 16, 2021, search warrant based upon "a facially insufficient application" because it "wholly failed to establish probable cause to believe that these four files were contraband." (Filing No. 39 at pp. 6-7). Defendant argues that the good faith exception does not apply due to the *Franks* violations and because the supporting affidavit was so lacking in indicia of probable cause as to render official belief in its existence entirely

unreasonable and the warrant was so facially deficient that the executing officer could not reasonably presume its validity. (Filing No. 38 at p. 4).

To be constitutionally valid, "a search warrant must be supported by a showing of probable cause." *United States v. Summage*, 481 F.3d 1075, 1077 (8th Cir. 2007). Probable cause exists if, based on the totality of the circumstances, a showing can be made "sufficient to create a fair probability that evidence of a crime will be found in the place to be searched." *United States v. Gabrio*, 295 F.3d 880, 883 (8th Cir. 2002) (internal quotation omitted). "Probable cause to issue a search warrant exists when an affidavit in support of the warrant sets forth sufficient facts to establish that there is a fair probability that contraband or evidence of criminal activity will be found in the particular place to be searched." *United States. v. Proell*, 485 F.3d 427, 430 (8th Cir. 2007) (quotation omitted). When relying on an affidavit to establish probable cause, "the probable cause determination must be based upon only that information which is found within the four corners of the affidavit." *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009). "Search warrant [a]pplications and affidavits should be read with common sense and not in a grudging, hyper technical fashion." *United States v. Ryan*, 293 F.3d 1059, 1061 (8th Cir. 2002) (quotations and citations omitted). An issuing judge's determination of probable cause "should be paid great deference by reviewing courts." *United States v. Mutschelknaus*, 592 F.3d 826, 828 (8th Cir. 2010).

Defendant asserts the March 16 warrant application wholly fails to establish probable cause to search all four files because the application only provided the information "that only one of the files had (maybe) matched a hash value" and "contained no information about the other three files." (Filing No. 39 at p. 7). Defendant further points out that the application only states it was "assumed . . . Facebook relied on the hash value match to identify the Child Sexual Exploitation Material," a term which is not defined to confirm whether the phrase "is the same, greater, or smaller than 18 U.S.C. § 2256's definition of 'child pornography,'" and without explaining the process, parameters of, or methodology of Facebook's hash-value search. Nor did the application describe the "known" image – i.e., the "image retained in the databases of Facebook, NCMEC, and/or law enforcement – to which (one of) the files had matched or state that the known file was confirmed child pornography." (Filing No. 39 at p. 7).

Defendant raises some valid criticisms of the March 16 warrant application. The deficiencies in the application cited by Defendant could have been corrected before the warrant

was issued. Nevertheless, given the deference to be paid to the issuing judge and the "common sense" reading to be given to warrant applications, the undersigned magistrate judge finds that the probable cause threshold was met. The warrant application provided the information that Facebook submitted a CyberTipline Report on October 20, 2020, to NCMEC. The CyberTip was provided due to a hash value match "on at least one digital image attached to an electronic message sent to an identified Facebook Messenger account," and identified the specific hashed file. The warrant application noted Facebook did not provide information whether it viewed the contents of the uploaded file, and thus it was "assumed" Facebook "relied on the hash value match to identify the Child Sexual Exploitation Material."

The warrant application provided the information that Facebook "maintains a database of hash values for files that Facebook has determined constitute child pornography, and uses that database to automatically compare files that are sent through a Facebook account," and explains, "A hash value is an alphanumeric sequence that is unique to a specific digital file. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Consequently, once a file has been 'hashed,' a suspected copy can be determined to be identical to the original file if it has the same hash value as the original, and not to be identical if it has a different hash value." The warrant application then explained what Facebook does after detecting a file on its servers "with the same hash value of a file from its database of known child pornography[.]" The application then identifies the Facebook user as Defendant, along with his information and birthdate, and the information that the Nebraska State Patrol submitted a subpoena to Defendant's phone service provider regarding the phone number associated with the Facebook account.

The application did rather somewhat confusingly state that the affiant officer "will not describe . . . the result of the NCMEC and [law enforcement] review of the images" and asked the court to "draw no inferences from the fact that [NCMEC and/or law enforcement] opened and viewed the electronic mail message and the attachment(s)," as the testimony from the affiant officer and declaration from NCMEC both were consistent that neither one opened and viewed the attachments. (TR. 52; Ex. 7 at p. 3). Regardless, this statement does not weigh in favor or against probable cause because nothing about the images was provided in the application.

Courts have equated hash-value matches to "digital fingerprints." See, e.g., *United States v. Miller*, 982 F.3d 412, 430 (6th Cir. 2020); *Ackerman*, 831 F.3d at 1294; *United States v.*

Wellman, 663 F.3d 224, 226 n.2 (4th Cir. 2011). A retrieved file's "hash value," is "essentially a particular file's digital signature, with the hash values of files known to contain child pornography. When the values match, investigators can pretty much be assured that the file at issue contains child pornography." *United States v. Shipton*, 5 F.4th 933, 935 (8th Cir. 2021); see also *United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008) (determining hash values established probable cause for a search warrant on the record). As set forth in the warrant application, Facebook maintains a database of hash values for files that Facebook has determined constitute child pornography, a hash value is unique to a specific digital file and any identical copy of the file will have exactly the same hash value as the original, Facebook identified by hash value match at least one digital image attached to an electronic message matching child sexual exploitation material from its database of known child pornography and forwarded the file to NCMEC, and that the user of the Facebook account had been identified as Defendant. This information established that there is a fair probability that contraband or evidence of criminal activity would be found in the four files sent from Facebook to NCMEC.

Defendant argues that the good faith exception does not apply due to the *Franks* violation and because the supporting affidavit was so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable and the warrant was so facially deficient that the executing officer could not reasonably presume its validity. (Filing No. 38 at p. 4). "Under [*United States v. Leon*, 468 U.S. 897, 920 (1984)], evidence obtained from a search performed under a warrant is suppressed only if '(1) the affiant [misled] the issuing judge with a knowing or reckless false statement; (2) the issuing judge wholly abandoned her judicial role; (3) the supporting affidavit was 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable'; or (4) the warrant was 'so facially deficient' that the executing officer could not reasonably presume its validity." *United States v. Hay*, 46 F.4th 746, 751 (8th Cir. 2022). "In the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause." *United States v. Leon*, 468 U.S. 897, 920 (1984).

As discussed above, the undersigned magistrate judge finds Sergeant Skaar did not act recklessly or intentionally in omitting certain information from his March 16 warrant application, thereby misleading the issuing judge. The undersigned magistrate judge further finds that, even if

the warrant application did not establish probable cause, Sergeant Skaar was not "entirely unreasonable" in his belief that the warrant was supported by probable cause, nor was the warrant so deficient that he "could not reasonably presume its validity." When Sergeant Skaar applied for the March 16 search warrants, he had the information that Facebook identified by hash value match at least one digital image attached to an electronic message matching child sexual exploitation material from its database of known child pornography, which it forwarded the file to NCMEC. Courts have established that when hash values match, "investigators can pretty much be assured that the file at issue contains child pornography." *United States v. Shipton*, 5 F.4th 933, 935 (8th Cir. 2021). Then, rather than open and review the hash matched file prior to obtaining a warrant (which some courts have seemingly authorized, see *Reddick*, 900 F.3d at 639), he applied for a warrant to "unlock" the files. Given the courts' view of the reliability of hash matching, Sergeant Skaar was not unreasonable in relying on the warrant under these circumstances.

c. March 31, 2021, warrant application

Defendant primarily argues the March 31, 2021, warrant application was based upon the information obtained from the invalid March 16, 2021, warrant. (Filing No. 39 at p. 9). Having rejected that argument, the undersigned magistrate judge finds no basis upon which to suppress evidence obtained from the March 31, 2021, warrant. Among other information, the March 31 warrant application included the affiant officer's review of the files from Defendant's Facebook account pursuant to the March 16 warrant, one of which was a video of a 10 to 12-year old female child engaging in a sexually explicit act. (Ex. 3 at pp. 3-5). Regardless of whether additional information should have been added as argued by Defendant, possession of one file of child pornography is a felony offense, see 18 U.S.C. § 2252A(a)(5), and the warrant application clearly established probable cause to issue the warrant for Defendant's Facebook account.

III. Post-warrant Constitutional Challenges

Defendant also challenges the constitutionality of various aspects of his July 7, 2023, interview with two FBI agents at his place of work. Defendant contends his statements were involuntary due to the "language barrier, coupled with the agents' presence at [Defendant's] job," the warrantless seizure of his cell phone was without probable cause or consent, and his consent

to search his cell phone was similarly involuntary. (Filing No. 39 at pp. 10-14; Filing No. 58 at pp. 9-10).[4]

a. Voluntariness of statements

"Statements to law enforcement authorities are voluntary if they are "'the product of an essentially free and unconstrained choice by [their] maker.'" *United States v. Vinton*, 631 F.3d 476, 482 (8th Cir. 2011) (quoting *Schneckloth v. Bustamonte*, 412 U.S. 218, 225 (1973)). "A statement is involuntary when it is extracted by threats, violence, or express or implied promises sufficient to overbear the defendant's will and critically impair his capacity for self-determination." *United States v. Roberts*, 975 F.3d 709, 718 (8th Cir. 2020). A court determines "if a defendant's will has been overborne by examining the totality of the circumstances, including both the conduct of law enforcement in exerting pressure to confess on the defendant and the defendant's ability to resist that pressure." *United States v. Sandell*, 27 F.4th 625, 630 (8th Cir. 2022) (quoting *United States v. Magallon*, 984 F.3d 1263, 1284 (8th Cir. 2021)). "[T]he degree of police coercion, the length of the interrogation, its location, its continuity, and the defendant's maturity, education, physical condition, and mental condition" are all relevant factors. *Magallon*, 984 F.3d at 1284 (quoting *United States v. Boslau*, 632 F.3d 422, 428 (8th Cir. 2011)). "The government must prove by a preponderance of the evidence that the defendant's statements were voluntary." *United States v. Brave Heart*, 397 F.3d 1035, 1040 (8th Cir. 2005).

After review of SA Wright's testimony and the audio recording of Defendant's interview, the undersigned magistrate judge finds that the totality of circumstances demonstrates that Defendant's statements clearly were voluntary and that his will was not overborne at any time he was talking to the agents. The agents first made contact with Defendant in a public place in the afternoon. The agents were wearing plain clothes and drove an unmarked vehicle. At the outset, SA Wright advised Defendant that he was free to leave and that he was not required to talk to

[4] Defendant separately argues that his July 7, 2023, statements and cell phone contents should be suppressed as fruit of the asserted Fourth Amendment violations surrounding the October 2020 CyberTip and March 2021 warrants under *Wong Sun v. United States*, 371 U.S. 471 (1963). (Filing No. 39 at p. 10). Although the Government does not raise this point, given the more than two-year gap between the execution of the purportedly defective search warrants and Defendant's non-custodial interview with different law enforcement officers, the undersigned magistrate judge finds that, even if a Fourth Amendment violation occurred in 2021, Defendant's July 2023 non-custodial interview was sufficiently attenuated such that it need not be suppressed as fruit of the earlier violation. See, e.g., *United States v. Riesselman*, 646 F.3d 1072, 1079 (8th Cir. 2011) (evidence must be suppressed only if the "illegality is at least a but-for cause of obtaining the evidence.").

them. SA Wright was accompanied by a Spanish-speaking agent, but during the course of the interview it was apparent that Defendant understood and spoke English. Review of the audio demonstrates SA Wright and Defendant spoke in English in conversational tones, and at no point did the agents raise their voices, yell, threaten, intimidate, or otherwise use violence to coerce Defendant into speaking. The interview took place in Defendant's employee breakroom, and the agents sat at the table with Defendant without blocking the breakroom door. SA Wright was forthcoming with Defendant, and repeatedly reassured Defendant he was not going to jail that day; nor was Defendant physically restrained or otherwise formally arrested at any point before or after the interview. The length of the interview was also relatively brief. Approximately 40-minutes into the interview, Defendant indicated he needed to help his coworkers close the business for the day, which the agents permitted. After an approximately 10-minute break, Defendant reapproached the agents, who were standing outside nowhere near Defendant's vehicle, to resume speaking to the agents for another twenty minutes. The totality of the above circumstances, including the length of the interview, its location, continuity, and lack of police coercion, all support a finding of voluntariness.

Defendant's personal characteristics also do not support a finding his "will and capacity for self-determination" were overborne at any point during his interactions with law enforcement officers. *United States v. LeBrun*, 363 F.3d 715, 726 (8th Cir. 2004) (calling this standard "very demanding"). Defendant was at work and did not appear to be intoxicated or under the influence of any substances, was in his 50s or 60s, and told SA Wright he had a college degree. Despite his assertion there was a "language barrier," review of the interview demonstrates Defendant understood SA Wright's questions and the nature of SA Wright's investigation, answered appropriately, and indicated he can read, "Otherwise I'd be working in a factory." Under these facts, the undersigned magistrate judge finds Defendant voluntarily made statements to law enforcement.

b. Seizure of Defendant's cell phone and his consent to search

Defendant argues he did not consent to the warrantless seizure of his cell phone. The government fails to address this point in its brief, only addressing Defendant's consent to the search of his cell phone. (Filing No. 53). Defendant appears to suggest that the warrantless seizure of his

cell phone led to his "defeatism and acquiescence" to SA Wright's separate request for consent to search the phone. (Filing No. 58 at p. 10).

SA Wright took Defendant's cell phone after Defendant voluntarily produced his cell phone during the interview and showed the interviewing officers apparent child pornography. SA Wright thus had probable cause to believe Defendant's cell phone contained evidence of a crime. See *United States v. Shrum*, 59 F.4th 968, 972 (8th Cir.), *cert. denied*, 144 S. Ct. 300 (2023) ("The officers had probable cause to believe [the defendant's] phone contained contraband or evidence of a crime" after the investigating officer "had seen photos of text messages between A.B. and [the defendant] that indicated they had [recently] engaged in sexual activity," and "There was a fair probability that those text messages, or related evidence of unlawful conduct, would be found on [the defendant's] phone.").

Not long thereafter, and during the same interview, Defendant provided consent to search his cell phone. Defendant argues this consent to the search of his cell phone was also involuntary. "The voluntariness of consent is assessed under the totality of the circumstances." *United States v. Thomas*, 97 F.4th 1139, 1142 (8th Cir. 2024) (citing *United States v. Chaidez*, 906 F.2d 377, 380 (8th Cir. 1990)). Consent is voluntary if it was "the product of an essentially free and unconstrained choice" by its maker. *Schneckloth v. Bustamonte*, 412 U.S. 218, 225 (1973). When determining whether consent was voluntary, the court "consider[s] factors, including the individual's age, intelligence and education, whether she cooperates with police, her knowledge of the right to refuse consent, whether the police threatened or intimidated her, and whether consent occurred in a public or secluded area." *Thomas*, 97 F.4th at 1142 (citing *United States v. Bearden*, 780 F.3d 887, 895 (8th Cir. 2015)). The court should also consider "whether the individual was intoxicated or under the influence of drugs, whether she relied on promises or misrepresentations made by the police, whether she was in custody or under arrest, and whether the individual objected to the search or stood silently while it occurred." *Id.* at 1143 (citing *Chaidez*, 906 F.2d at 381).

For many of the same reasons discussed above when concluding Defendant's statements were voluntary, the undersigned magistrate judge also finds the totality of the circumstances demonstrates Defendant's consent to the search of his cell phone was voluntary. As outlined above, the FBI agents' interaction and interview with Defendant was conversational, took place at his place of work and was not police dominated, involved no threats, promises, or intimidation, Defendant was not physically restrained or arrested, and Defendant asked for and was given time

to take a break after approximately 40 minutes of conversation. SA Wright asked Defendant if he would be "willing to sign a form to let me search your phone," but Defendant hesitated because he "really need[s]" his phone. Rather than forcing the issue, SA Wright replied, "It's your decision," and informed Defendant that giving such consent would not lead to him getting his phone back sooner. (Ex. 4 at 41:05-42:36; TR. 66-67). SA Wright testified he advised Defendant "multiple times" he was free to decline consent to search, and that providing consent "would not get his phone back quicker." (TR. 66-67). Defendant asked SA Wright if he was charged with something and expressed concern about losing his job, and SA Wright replied, "that's tough to tell" and will "largely . . . depend on what else we find on the phone." (Ex. 4 at 44:48-45:40). After Defendant reinitiated contact with the agents outside in the parking lot, SA Wright circled back to Defendant's consent to search his phone, asking "Is that something you want to give me?" (Ex. 4 at 1:08). SA Wright repeatedly corrected Defendant's belief that because SA Wright had the phone, he could search the phone, explaining that without consent, he would have to get a search warrant that a judge "signs off on," and that taking Defendant's phone is different from searching his phone and he "can't look at it" without consent or a warrant. SA Wright continued, "I need you to give me consent to say I can look at it, or I need to go get a search warrant from a judge." Defendant responded, "I'll sign it, whatever" and repeated, "You already got it," referring to SA Wright's seizure of the phone; SA Wright again clarified, "I got it, but I can't search it." (Ex. 4 at 1:08-1:09:40).

Based on Defendant's indication that he would "sign it," SA Wright prepared a Form FD-597 property receipt for Defendant's cell phone, explaining the form's purpose and explained it is not the consent form, and separately provided and explained the Form FD-941 consent to search computers or cell phones form. SA Wright read the consent form to Defendant, and summarized, "In short it's saying that you are giving the FBI consent to search this phone and take any evidence that we find in it. If you consent to that, you sign right there." Defendant then signed the form consenting to the search of his Samsung Galaxy cell phone. The surrounding circumstances and Defendant's personal characteristics both weigh in favor of voluntariness of this consent. Defendant provided this consent during a non-custodial interview in the parking lot of his workplace; SA Wright read the consent form out lout and was provided an opportunity to read and sign the consent form without inducement or pressure from law enforcement; his consent was obtained just over an hour after the agents first made contact with him; Defendant was not

restrained or formally arrested; he was not threatened, intimidated, coerced, promised anything, or misled; he was not intoxicated; and he was a 50 to 60 year old man with a college degree who had conversed with the agents in English without issue. Under these facts, the totality of the circumstances demonstrate Defendant's consent to search was also voluntary. See *Thomas*, 97 F.4th at 1142.

Upon consideration,

IT IS HEREBY RECOMMENDED to Robert F. Rossiter, Jr., Chief United States District Court Judge, that Defendant's Motion to Suppress and Request for Hearing, and Motion for a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), (Filing No. 38) be denied.

Dated this 16th day of April, 2025.

BY THE COURT:

s/Michael D. Nelson
United States Magistrate Judge

ADMONITION

Pursuant to NECrimR 59.2, any objection to this Findings and Recommendation shall be filed with the Clerk of the Court within fourteen (14) days after being served with a copy of this Findings and Recommendation. Failure to timely object may constitute a waiver of any such objection. The brief in support of any objection shall be filed at the time of filing such objection. Failure to file a brief in support of any objection may be deemed an abandonment of the objection.